Kristin Cornuelle
kcornuelle@orrick.com (Bar No. 130922)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1120 NW Couch Street, Suite 200
Portland, OR 97209
Telephone: (503) 943-4800
Facsimile: (503) 943-4801

Attorneys for Plaintiff WELLS FARGO ADVISORS FINANCIAL NETWORK LLC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

WELLS FARGO ADVISORS FINANCIAL NETWORK LLC Plaintiff, **v.** **JOHN DOES (1 THROUGH 10)**, Defendants.	No. 3:17-cv-1861 **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Wells Fargo Advisors Financial Network LLC ("WFAFN" or "Plaintiff") hereby complains and alleges against JOHN DOES 1 through 10 (collectively "Defendants" or "John Does") as follows:

NATURE OF THE ACTION

1. This action is based on: (1) the Computer Fraud and Abuse Act, 18 U.S.C. 1030, *et seq.*; (2) Oregon's Computer Crime Statute, Or. Rev. Stat. Ann. § 164.377 (2017); (3) conversion; and (4) unfair competition. Plaintiff seeks injunctive relief, damages, and other appropriate relief to stop Defendants' unauthorized access to confidential information and to stop Defendants' use, disclosure, and misappropriation of confidential information.

THE PARTIES

2. WFAFN is a subsidiary of Wells Fargo & Company. WFAFN has its principal place of business in St. Louis, Missouri. WFAFN offered product offerings and services through Third-Party Steinberg Investment Group, LLC ("SIG") to its clients. Along with its product offerings and services, WFAFN also provided SIG with IT safety protocols and guidelines that SIG was required to use in the operation of its business. During all relevant times, third-parties SIG and Lance Steinberg ("Mr. Steinberg") were independent contractors for WFAFN and held themselves out as a WFAFN financial advisor.

3. Third-Party Lance Steinberg ("Mr. Steinberg") is an individual residing in Portland, Oregon. Mr. Steinberg is the owner and President of Third-Party SIG, which is located at One SW Columbia Street, Portland, Oregon 97258. Mr. Steinberg and SIG were independent contractors of WFAFN.

4. Third party GoDaddy, Inc. ("GoDaddy") is a technology company that offers Internet-related services, including Internet hosting services, email accounts, Internet domains, and cloud storage. GoDaddy has offices at 1020 Enterprise Way, No. 300, Sunnyvale, California 94089. As described herein, GoDaddy is the registrar for the Internet domain www.steinberginvestmentgroup.com (the "SIG Internet Domain") and maintains the associated

email server @Steinberginvestmentgroup.com (the "SIG Email Server") that Mr. Steinberg and SIG use to conduct business in Portland.

5. Third party Zoho Corporation ("Zoho") is a technology company that offers Internet-related services, including email services. Zoho has offices at 414 Hacienda Drive, Pleasanton, California 94588. As described herein, Defendants used an email server that they maintain through Zoho to divert emails from the SIG Email Server.

6. Plaintiff is unaware of the true name and capacity of Defendants sued herein as JOHN DOES 1 through 10, and therefore sues them by such fictitious name. Plaintiff is informed and believes and therefore alleges that Defendants have, without authorization or exceeding their authorization, accessed Mr. Steinberg's business computer (the "SIG Business Computer") and diverted from the SIG Email Sever emails that contain confidential business information to an email server that Defendants maintain through Zoho. Plaintiff will amend its complaint to allege Defendants' true names and capacities when ascertained. Plaintiff is informed and believes and therefore alleges that the fictitiously named Defendants are responsible in some manner for the occurrences herein alleged, and that Plaintiff's injuries that are herein alleged were proximately caused by such Defendants.

JURISIDICTION AND VENUE

7. This is a Complaint for an injunction, damages, and other appropriate relief stemming from Defendants' unauthorized access of the SIG Business Computer and Defendants' unauthorized diversion of emails containing confidential business information from the SIG Email Server to an email server Defendants maintain. In this action, Plaintiff asserts violations of the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030, *et seq.*); violation of Oregon's Computer Crime Statute (Or. Rev. Stat. Ann. § 164.377); common law conversion and unfair competition; and declaratory relief against Defendants.

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331. This action also arises from Defendants' violation of Oregon statutory law and common law.

Accordingly, this Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b), as a substantial part of the events or omissions giving rise to the claims pleaded herein occurred in the District of Oregon. Specifically, Mr. Steinberg is a resident of Portland, Oregon and as described herein, operates SIG in Portland, Oregon. Moreover, at all relevant times, the SIG Business Computer was located in Portland, Oregon.

NATURE OF MR. STEINBERG'S BUSINESS

10. Mr. Steinberg is the owner and President of SIG, a Portland-based firm committed to providing personalized investment and wealth management services to each of its clients. SIG customizes each of its clients' investment plans to their specific situation, which incorporates their long-term goals and objectives. In order to offer these services to its clients, SIG offered investment products and services through WFAFN. Mr. Steinberg and SIG were WFAFN independent contractors, from October 1, 2011 through November 2, 2017 WFAFN provided Mr. Steinberg with IT safety protocols and guidelines that SIG was required to use in the operation of its business in order to protect the SIG Business Computer from, among other things, unauthorized access by third parties.

11. In order to operate SIG, Mr. Steinberg registered and maintains the custom Internet domain www.steinberginvestmentgroup.com. Mr. Steinberg also created and maintains a business email server at @Steinberginvestmentgroup.com (the "SIG email address"), which he uses to communicate with his clients. In particular, the SIG email address is an outward facing email address by which clients can send emails to SIG and Mr. Steinberg. Emails incoming through the SIG email address are redirected to a WFAFN-email account WFAFN provided to Mr. Steinberg. Mr. Steinberg registered the SIG Internet Domain and SIG Email Server through GoDaddy. At all relevant times, Mr. Steinberg kept the SIG Business Computer—which is a desktop—at SIG's offices in Portland, Oregon.

MR. STEINBERG'S CONFIDENTIAL BUSINESS INFORMATION

12. Mr. Steinberg and SIG took reasonable and appropriate steps in protecting its confidential business information (including communications with clients), and limiting access to sensitive confidential business information. The SIG Business Computer is password-protected and uses anti-virus software programs to maintain its security. The SIG email account is also password-protected. Only Mr. Steinberg and his assistant had access to SIG Business Computer. Mr. Steinberg also maintained a separate password with which to access the SIG email account through the SIG Business Computer. SIG's offices remained locked during non-business hours and are not accessible to the public. During business hours, members of the public were not allowed into the SIG offices without being accompanied by Mr. Steinberg or his assistant.

DEFENDANTS' UNLAWFUL CONDUCT

13. As discussed herein, on or about April 2, 2017, Defendants accessed the SIG Business Computer without authorization. In so doing, Defendants gained access to Mr. Steinberg's GoDaddy account and were able to change critical account information that allowed them to redirect email traffic away from the SIG Email Server to an email server Defendants maintained through Zoho.

14. Beginning on or about April 2, 2017, Mr. Steinberg began experiencing unusual activity related to his online personal accounts. On April 2, 2017, after returning home from traveling, Mr. Steinberg received a telephone call purporting to relate to his personal online account with Amazon in which he was asked about resetting his password. At that time, Mr. Steinberg had not taken steps to change the password to his Amazon account; nor had Mr. Steinberg accessed his Amazon account recently. Believing the telephone call may have been a hoax, Mr. Steinberg did not take steps to reset the password to his Amazon account.

15. On April 3, 2017, Mr. Steinberg returned to the SIG office. Upon returning to his office, Mr. Steinberg logged onto the SIG Business Computer and discovered multiple open Internet browsing sessions, including open browsing sessions for his online personal account

with Capital One and his online personal account with Amazon. Neither Mr. Steinberg nor his assistant had started Internet browsing sessions for either Capital One or Amazon.

16. By late morning of April 3, 2017, Mr. Steinberg had noticed that he was not receiving emails from clients at the SIG email address that is managed through the SIG Email Server. That afternoon, in light of the lack of incoming emails, Mr. Steinberg sent a test email from his personal email account to the SIG email address to determine whether the SIG email account was active. By all indications, the test email was successfully sent from Mr. Steinberg's personal email account. However, there is no record of the SIG email account having received the test email.

17. During this time, a client contacted Mr. Steinberg regarding an email the client had sent to the SIG email address to which Mr. Steinberg had not responded. Mr. Steinberg had no record of receiving the email from the client. Given the lack of incoming outside emails to the SIG business email account and the suspicious activity regarding his personal online accounts, Mr. Steinberg and his assistant contacted GoDaddy to determine whether his GoDaddy account was still operational. Upon contacting GoDaddy, Mr. Steinberg learned that his GoDaddy account had been accessed on April 2, 2017 without his authorization. When Mr. Steinberg's GoDaddy account was accessed, critical account information was altered in order to redirect incomings emails from the SIG Email Server to an email server operated through Zoho.

18. Mr. Steinberg also notified WFAFN. WFAFN conducted an investigation and determined that the SIG Business Computer was remotely accessed on or about April 2, 2017 at approximately 2:09 p.m. (PST). According to the Internet Protocol ("IP") Address used to access the SIG Business Computer, it appears the access originated from a computer in the Dominican Republic. During that time, Mr. Steinberg had not traveled to the Dominican Republic.

19. The investigation further revealed that on April 2, 2017 at approximately 2:23 p.m. (PST), Mr. Steinberg's browser on the SIG Business Computer had been used to access Mr. Steinberg's account with GoDaddy. WFAFN and Mr. Steinberg worked to redirect the SIG

domain back to the SIG Email Server Mr. Steinberg originally set up. The investigation further revealed that Mr. Steinberg's personal Capital One and Amazon accounts were accessed on April 2, 2017 at approximately 2:39 p.m. (PST) and 2:41 p.m. (PST) respectively. Although the investigation revealed that Defendants gained unauthorized access to certain of Mr. Steinberg's personal information, there is no indication that the Defendants were able to obtain information regarding Mr. Steinberg's clients—as that information is not stored on the SIG Business Computer.

20. Defendants were not authorized to access the SIG Business Computer, Mr. Steinberg's GoDaddy account, or the SIG Email Server in order to redirect emails to Defendants' own email server they operated through Zoho. Any emails or information contained therein that Defendants obtained were obtained without authorization.

21. Defendants' unauthorized access to the SIG Business Computer, Mr. Steinberg's GoDaddy account, and the SIG Email Server caused irreparable harm to Plaintiff and caused Plaintiff to suffer damages, including impairment of the SIG Business Computer and the impairment of SIG's confidential business information, specifically the emails diverted from the SIG Email Server. Defendants' misconduct also caused Plaintiff to incur losses, including without limitation the costs associated with (a) investigating Defendants' unauthorized access; (b) conducting a damages assessment; and (c) taking mitigation measures.

22. Upon information and belief, Defendants profited from their unauthorized access to the SIG Business Computer, Mr. Steinberg's GoDaddy account, and SIG Email Server.

CLAIMS FOR RELIEF

FIRST CLAIMS FOR RELIEF

(Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(2)(c), (a)(4), and (a)(5))

23. Plaintiff realleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 22 above.

24. The SIG Business Computer that Mr. Steinberg used to manage the @Steinberginvestmentgroup.com email account is a "protected computer" within the scope of 18

U.S.C. § 1030(e)(2)(B) in that it is used in interstate commerce or communication—specifically the Internet.

25. On or about April 2, 2017, Defendants knowingly and intentionally accessed SIG's protected computer and Mr. Steinberg's GoDaddy account in order to divert email traffic away from the SIG Email Server to an email server that Defendants operate through Zoho. Defendants' unauthorized access of the SIG Business Computer and Mr. Steinberg's GoDaddy account caused damages and losses in excess of $5,000 in a one-year period, in that Defendants' conduct impaired the integrity of the SIG Business Computer that has caused Plaintiff to incur costs to investigate Defendants' unauthorized access and to repair and implement additional safety measures to prevent further unauthorized access by Defendants.

26. Defendants' intentional access to the SIG Business Computer and in turn Mr. Steinberg's GoDaddy account without authorization and/or exceeding authorization and subsequent redirection of email from the @steinberginvestmentgroup.com email address to their email server at Zoho violates 18 U.S.C. § 1030(a)(2)(c).

27. As a result of Defendants' intentional unauthorized access of the SIG Business Computer, Mr. Steinberg's GoDaddy account, and the redirection of email away from the SIG Email Server to an email server Defendants operate through Zoho, Defendants knowingly, or recklessly, caused damages and/or loss in violation of 18 U.S.C. § 1030(a)(5)(a)-(c).

28. Defendants knowingly and with intent to defraud, without authorization and/or in excess of authorization, accessed SIG's protected computer and by means of such conduct, furthered the intended fraud and obtained without payment services valued in excess of $5000 in a one-year period, within the scope of 18 U.S.C. § 1030(a)(4).

29. Pursuant to 18 U.S.C. § 1030(g), Plaintiff is entitled to compensatory damages and injunctive or equitable relief.

SECOND CLAIM FOR RELIEF

(Violation of Oregon's Computer Crime Statute, ORS § 164.377, § 161.625, § 161.635)

30. Plaintiff realleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 29 above.

31. On or before April 2, 2017, Defendants knowingly and intentionally accessed SIG's protected computer and Mr. Steinberg's GoDaddy account in order to divert email traffic away from the SIG Email Server to an email server that Defendants operate through Zoho. Defendants' access to SIG's protected computer was without authorization and/or exceeding any authorization from SIG or Mr. Steinberg, for the purpose of committing theft and/or executing a scheme or artifice to defraud in violation of O.R.S. § 164.377 (2).

32. Upon information and belief, Defendants knowingly and without authorization, accessed SIG's protected computer and email, and in so doing altered, damaged, and/or destroyed SIG's protected computer and email in violation of O.R.S. § 164.377 (3).

33. Defendants knowingly and without authorization, accessed SIG's protected computer in violation of O.R.S. § 164.377 (4).

34. Pursuant to O.R.S. § 164.377 (5)(a), § 161.625, § 161.635, Plaintiff is entitled to exemplary damages.

THIRD CLAIM FOR RELIEF

(Conversion)

35. Plaintiff realleges and incorporates by reference each and every allegation set forth in paragraphs 1 through 34 above.

36. Defendants knowingly and intentionally accessed, without authorization, the SIG Business Computer and Mr. Steinberg's GoDaddy account in order to divert emails away from the SIG Email Server to an email server that Defendants operated through Zoho.

37. Defendants intentionally exercised dominion and/or control over the SIG Business Computer and Mr. Steinberg's GoDaddy account, for example, by accessing the SIG Business Computer and Mr. Steinberg's GoDaddy account in order to divert email traffic away from the SIG Email Server to an email server Defendants operate through Zoho.

38. Defendants' intentional exercise of dominion and/or control over the SIG Business Computer and Mr. Steinberg's GoDaddy account seriously interfered with Mr. Steinberg's and SIG's right to control the SIG Business Computer, Mr. Steinberg's GoDaddy account, and the SIG Email Server. As a consequence, Plaintiff has been harmed because the SIG Business Computer, Mr. Steinberg's GoDaddy account, and the SIG Email Server Steinberg were compromised, in whole or part, and required remediation. For example, as a result of Defendants' actions, Mr. Steinberg can no longer use his SIG Business Computer as it has been quarantined.

FOURTH CLAIM FOR RELIEF

(Unfair Competition)

39. Plaintiff realleges and incorporate by reference each and every allegation set forth in paragraphs 1 through 38 above.

40. Plaintiff expended considerable time and money developing SIG's business into a trusted personalized investment and wealth management services firm.

41. Defendants accessed and/or obtained confidential business information from SIG without authorization and disclosed and/or used the information for Defendants' benefit.

42. As a consequence of Defendant's unauthorized access and/or disclosure of any such confidential business information, Plaintiff has been harmed, including reputational harm, and the loss of goodwill. Plaintiff is informed and believes, and on that basis alleges, that Defendants' conduct constitutes common law unfair competition and was carried out willfully, fraudulently, maliciously, and with wanton disregard of Plaintiff's rights, thereby entitling Plaintiff to compensatory and punitive damages to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendants, inclusive as follows:

1. For compensatory, consequential, and incidental damages according to proof;

2. For recovery of the unjust enrichment obtained by Defendants as a result of its wrongful conduct;

3. For exemplary damages as provided in O.R.S. § 164.377;

4. For preliminary and permanent injunctive relief, and/or an order of specific performance, commanding Defendants to cease and desist his/her unlawful conduct, including: their unauthorized access of the SIG Business Computer and the SIG Email Server;

5. For an audit by an independent third party verifying the removal of Plaintiff's information from any and all of Defendants' computers, servers, records, information systems and/or other storage facilities;

6. For an award of prejudgment interest and costs of suit to the extent permitted by law;

7. For an award of Plaintiff's reasonable attorneys' fees; and

8. For such other and further relief as the Court deems just and proper.

Dated: November 20, 2017

Respectfully submitted,

By: *__/s/ Kristin S. Cornuelle__*

Kristin S. Cornuelle
Email: kcornuelle@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1120 NW Couch Street, Suite 200
Portland, OR 97209
Telephone: (503) 943-4800
Facsimile: (503) 943-4801

Attorneys for Plaintiff
Wells Fargo Advisors Financial Network LLC